

SN3262 – Network Management & Security

RMON

Reading:

Leinwand, A. & Conroy, K. F. (1996) Network Management: A Practical Perspective 2nd ed.

Addison-Wesley. Chapter 11. (*Somewhat dated*).

Stallings, W. (1999) SNMP, SNMPv2, SNMPv3, and RMON 1 and 2. 3rd. ed. Reading Massachusetts, Addison-Wesley. Chapters 8, 9 & 10.

Remote Monitoring (Chapter 55 of Internetworking Technology Handbook).(2006) Cisco Systems [Internet] Available from

<http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/rmon.pdf>[Accessed 12 November 2008]

rfcs: rfc1513 (*Obsoleted*), rfc1757 (*Obsoleted*),

rfc2819 (Remote Network Monitoring Management Information Base),

rfc2613 (Remote Network Monitoring MIB Extensions for Switched Networks Version 1.0) and

rfc3577 (Introduction to the Remote Monitoring (RMON) Family of MIB Modules).

What is RMON?

- RMOM stands for remote monitoring.
- Monitors traffic on network segments.
- Originally it used stand-alone probes attached to a network segment. One probe per segment.
- Now it is incorporated into switches and routers.
- Originally (RMON 1) it gathered statistics at the data-link layer.
- Then came RMON 2 which allows the gathering of statistics at the network layer and above.
- It is now group 16 in MIB-2

Goals

- To gather statistics of remote network segments.
- Performing network management in network segments.

RMON Applications

- Offline operations: trace analysis
- Preemptive monitoring: continuous monitoring and notification (query-based and event-based)
- Problem detection and reporting: triggered filters
- Value-added Data: gathering important information such as the number of errors or traffic types
- Multiple Manager: it provides multiple views – e.g. different managers with different functions also added reliability.

Another mystery!

```
#!/bin/bash
let ifSpeed=200000000
let n=0

while [ $n -lt 10 ]
do
    let time1="$(snmpget -v2c -c docm_student dali 1.3.6.1.2.1.1.3.0 | gawk '{print $4}' | \
sed 's/(//' | sed 's/)//')"
    let in1="$(snmpget -v2c -c docm_student dali 1.3.6.1.2.1.2.2.1.10.2 | gawk '{print $4}')"
    let out1="$(snmpget -v2c -c docm_student dali 1.3.6.1.2.1.2.2.1.16.2 | gawk '{print $4}')"
    let time2="$(snmpget -v2c -c docm_student dali 1.3.6.1.2.1.1.3.0 | gawk '{print $4}' | \
sed 's/(//' | sed 's/)//')"

    let T1=$(((time1+time2)/2))
    let bytes1=$((in1+out1))

    sleep 30

    let time3="$(snmpget -v2c -c docm_student dali 1.3.6.1.2.1.1.3.0 | gawk '{print $4}' | \
sed 's/(//' | sed 's/)//')"
    let in2="$(snmpget -v2c -c docm_student dali 1.3.6.1.2.1.2.2.1.10.2 | gawk '{print $4}')"
    let out2="$(snmpget -v2c -c docm_student dali 1.3.6.1.2.1.2.2.1.16.2 | gawk '{print $4}')"
    let time4="$(snmpget -v2c -c docm_student dali 1.3.6.1.2.1.1.3.0 | gawk '{print $4}' | \
sed 's/(//' | sed 's/)//')"

    let T2=$(((time3+time4)/2))
    let time=$((T2-T1))
    let bytes2=$((in2+out2))
    let bits=$(((bytes2-bytes1)*8))
    let rate=$(((bits*100)/time))
    echo -n "At $(date +%H:%M:%S) the utilisation over the previous 30s was "
    echo "scale=3; $rate*100/$ifSpeed" | bc | gawk '{if($1<1) print "0"$1};{if($1>=1) print $1}'
    let n+=1
done
```

Output

```
At 09:27:51 the utilisation over the previous 30s was 0.096
At 09:28:21 the utilisation over the previous 30s was 0.277
At 09:28:52 the utilisation over the previous 30s was 0.139
At 09:29:22 the utilisation over the previous 30s was 0.007
At 09:29:53 the utilisation over the previous 30s was 0.007
At 09:30:23 the utilisation over the previous 30s was 0.008
At 09:30:54 the utilisation over the previous 30s was 0.012
At 09:31:24 the utilisation over the previous 30s was 0.006
At 09:31:54 the utilisation over the previous 30s was 0.016
At 09:32:25 the utilisation over the previous 30s was 0.014
```